

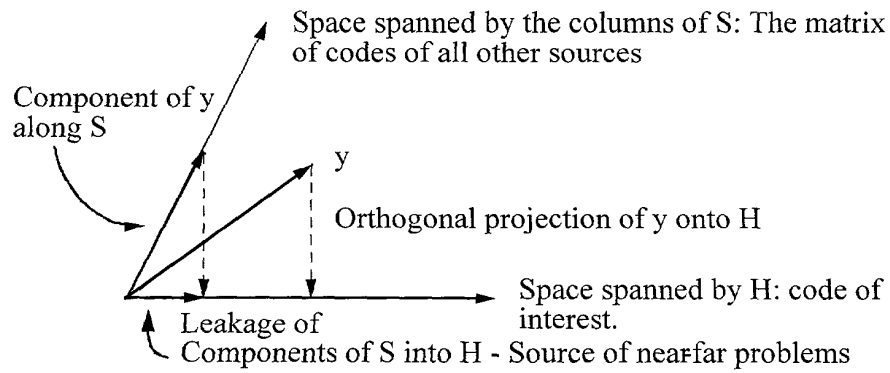
**FIG. 1****(PRIOR ART)**

FIG. 2

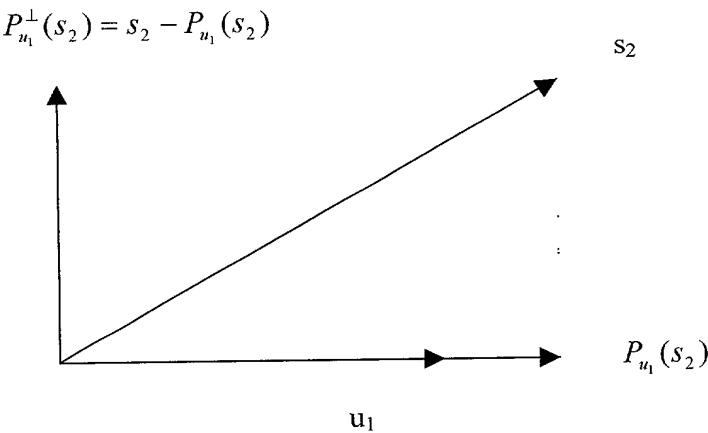


FIG. 3

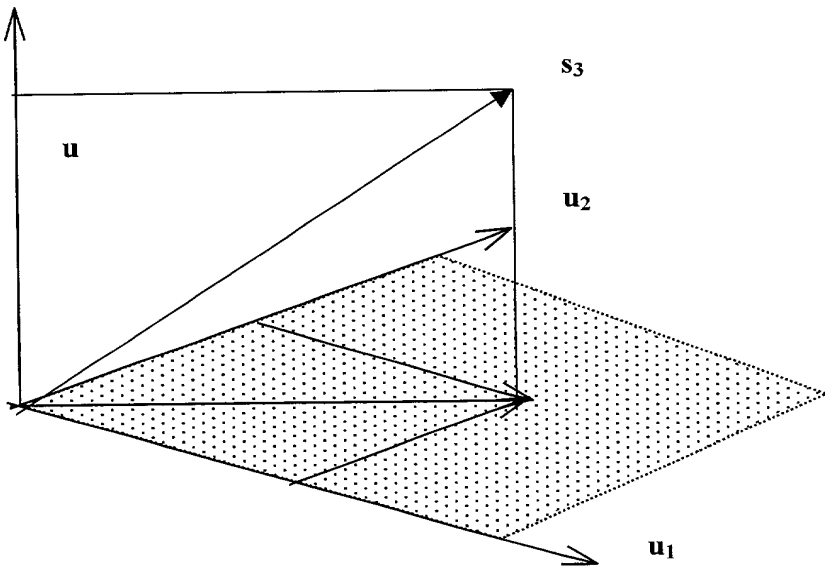


FIG. 4

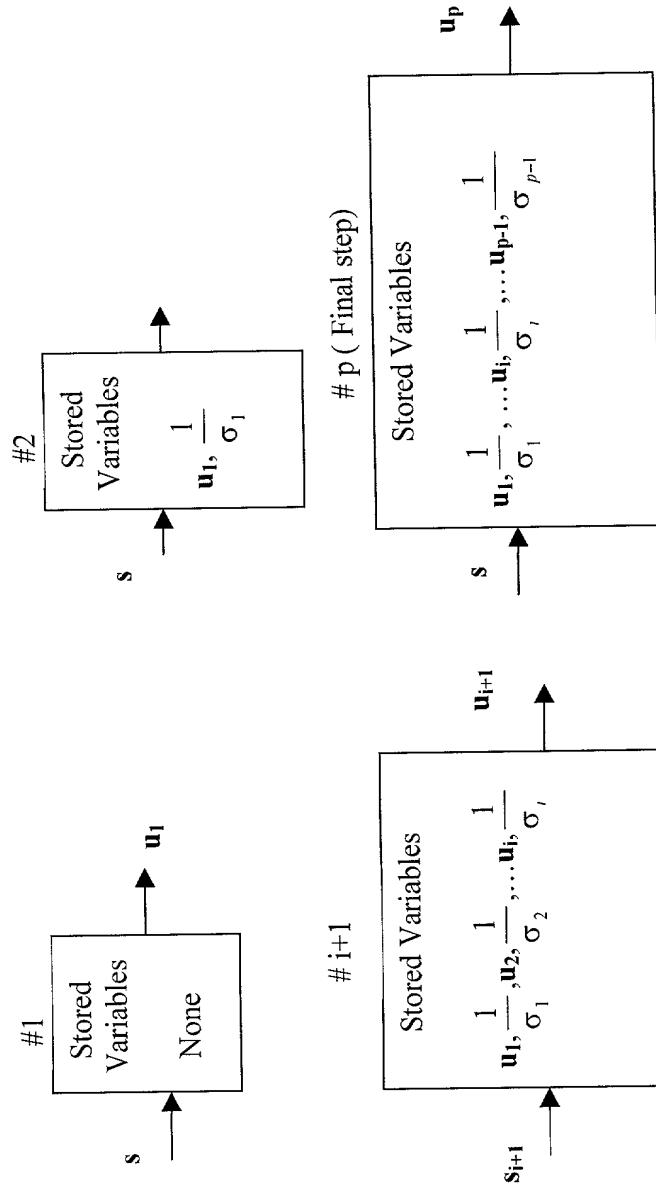


FIG. 5

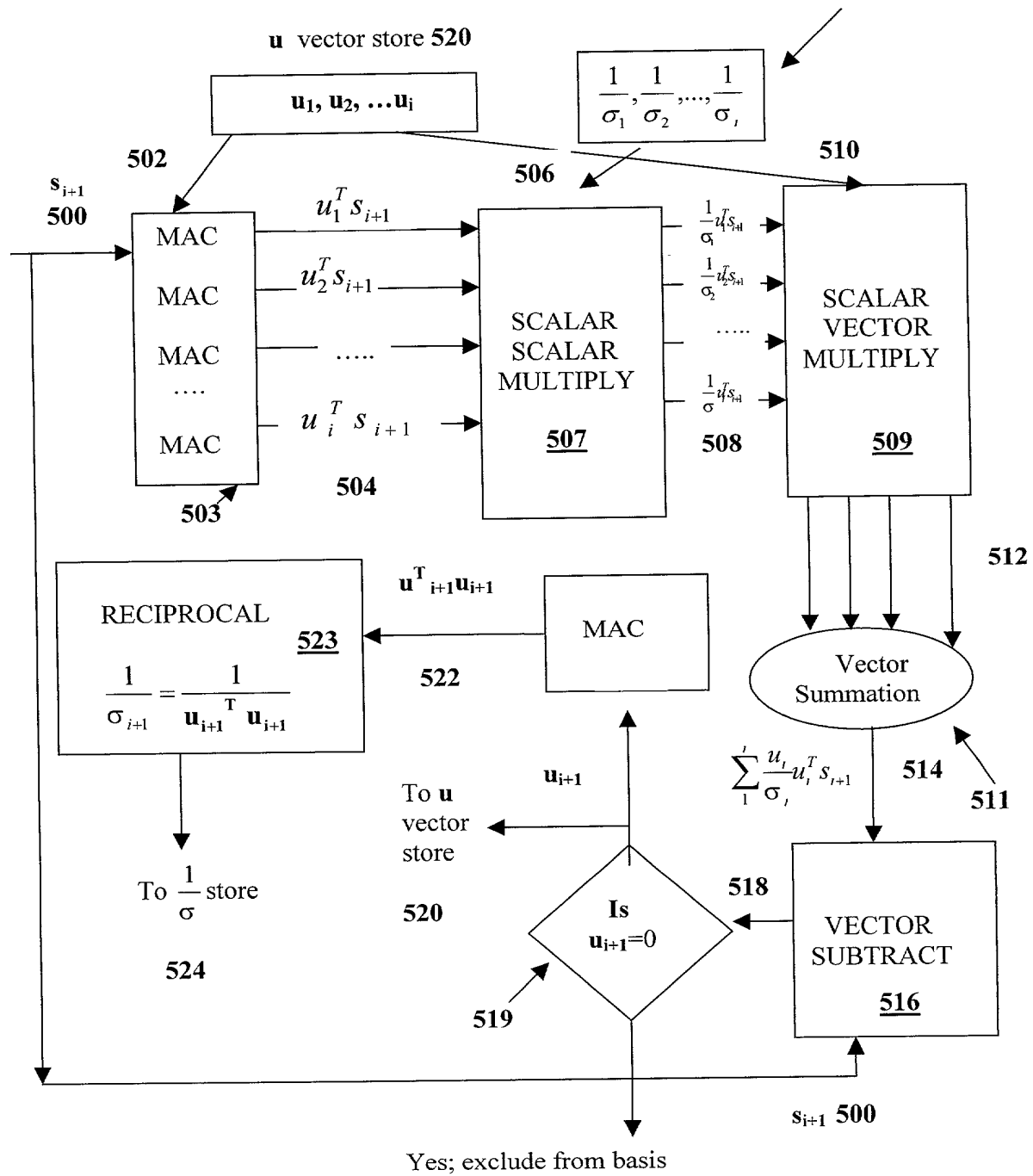


FIG. 6 is a block diagram of a MAC (Message Authentication Code) block 503. The block 503 receives two inputs:  $s_{i+1}$  and  $u_1, u_2, \dots, u_i$ . The output of the block 503 is  $u_1^T s_{i+1}, u_2^T s_{i+1}, \dots, u_i^T s_{i+1}$ .

FIG.6

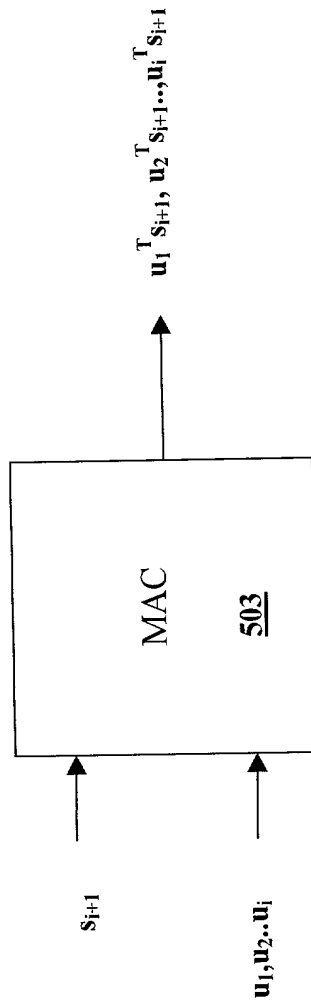


FIG.7

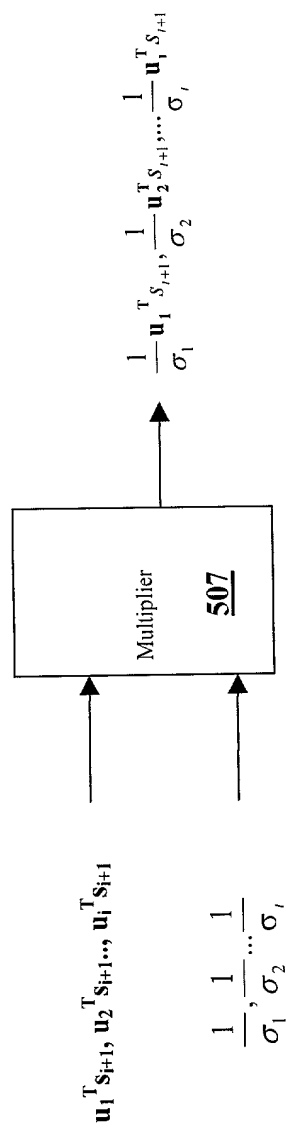


FIG.8

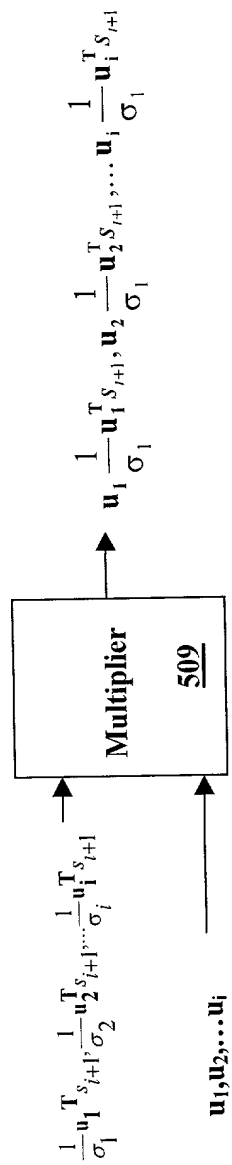




FIG.9

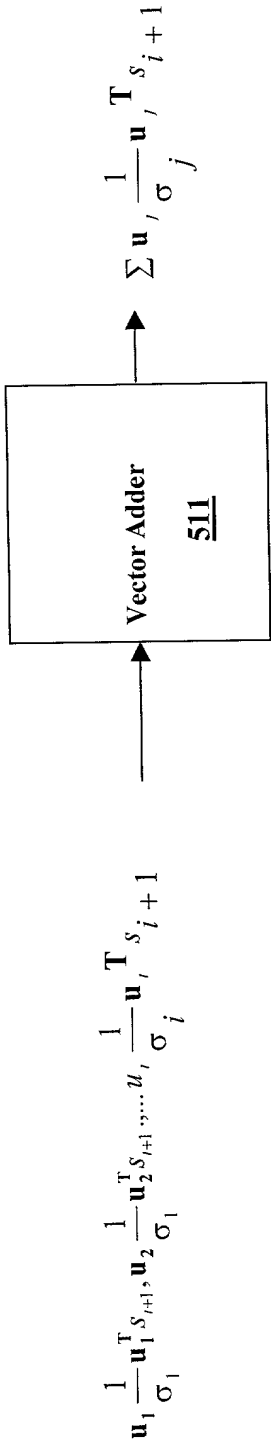


FIG. 10

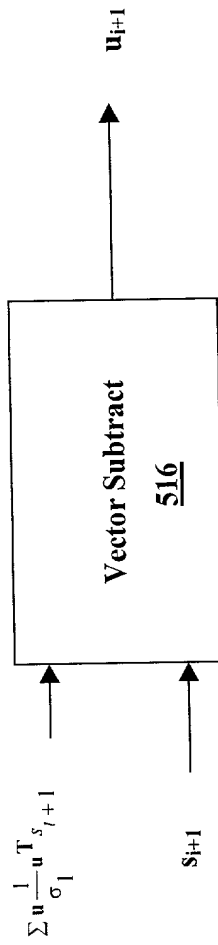


FIG. 11

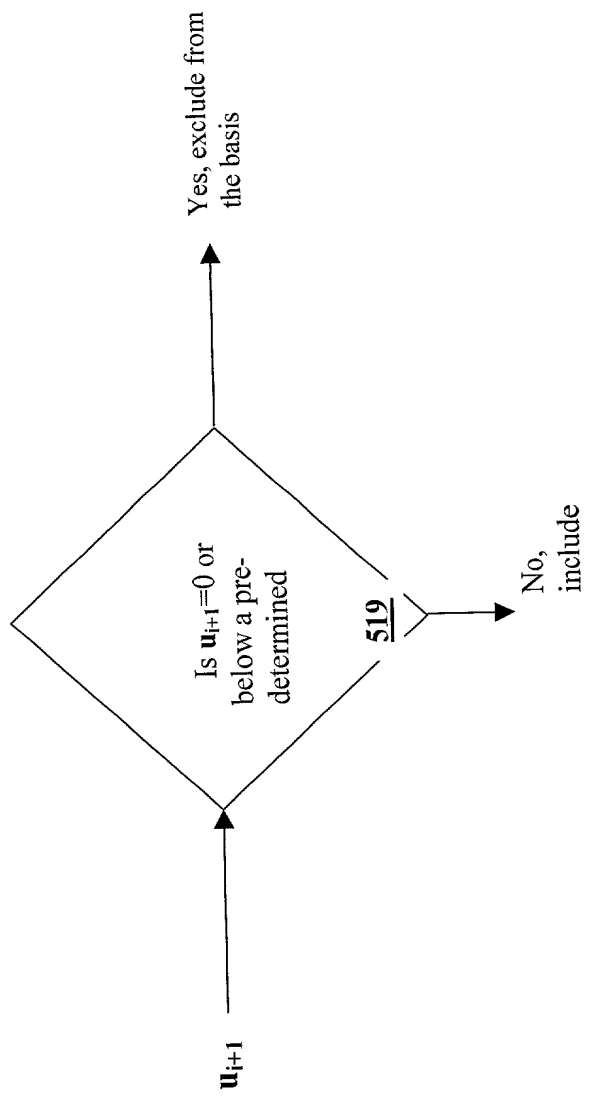


FIG. 12

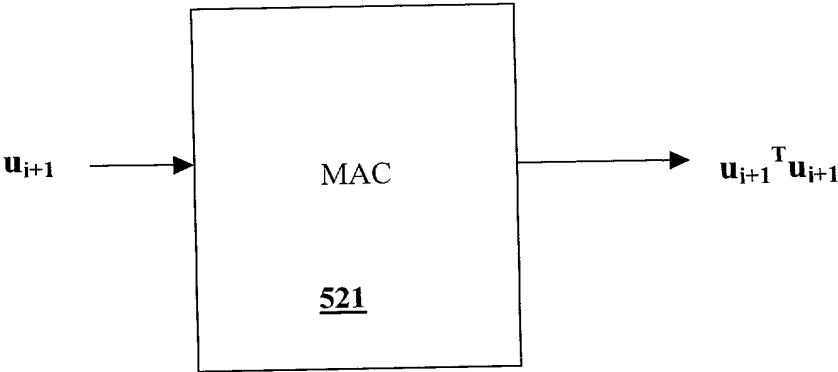


FIG. 12 is a block diagram of a MAC block 521. The MAC block 521 receives an input vector  $u_{i+1}$  and outputs a scalar value  $u_{i+1}^T u_{i+1}$ .

FIG. 13

FIG.13

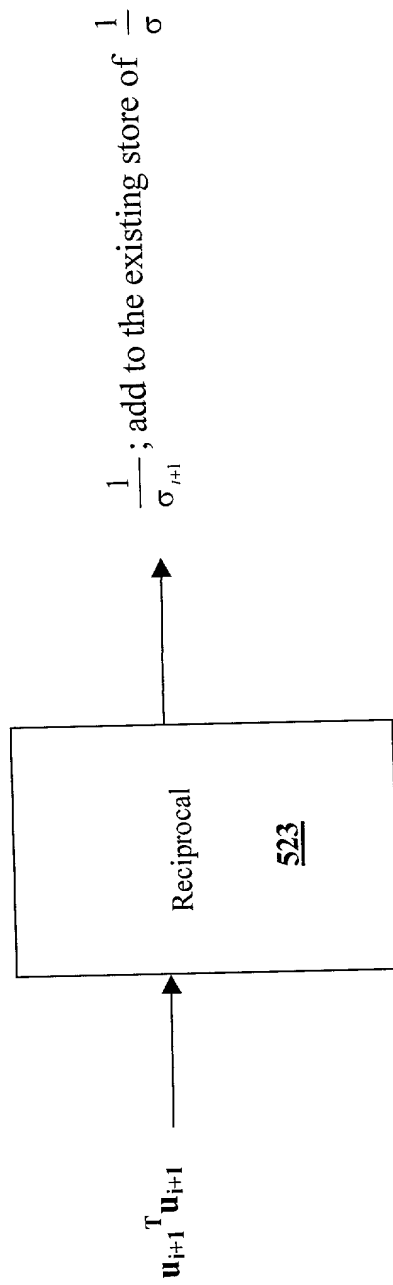


FIG. 14

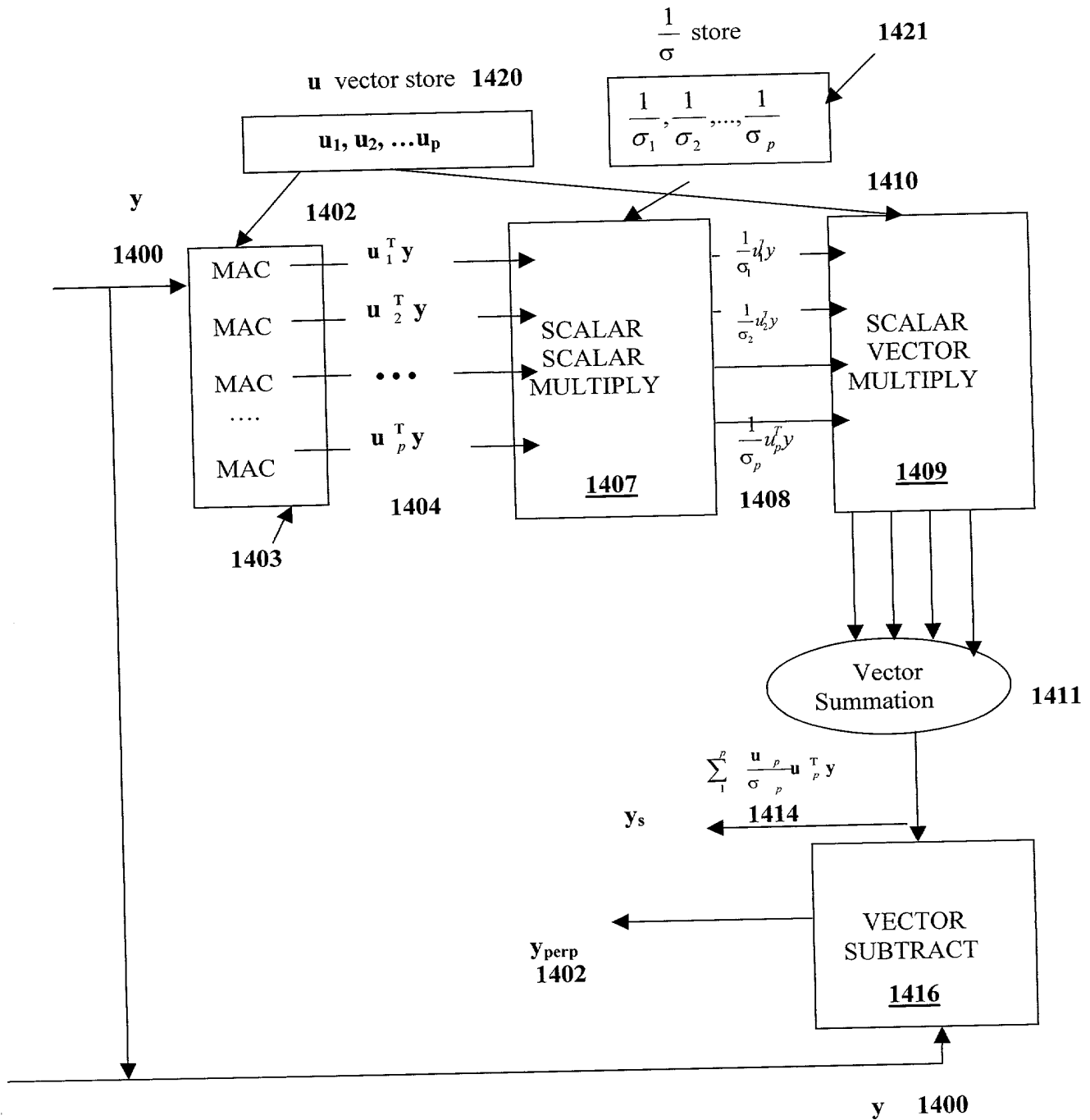
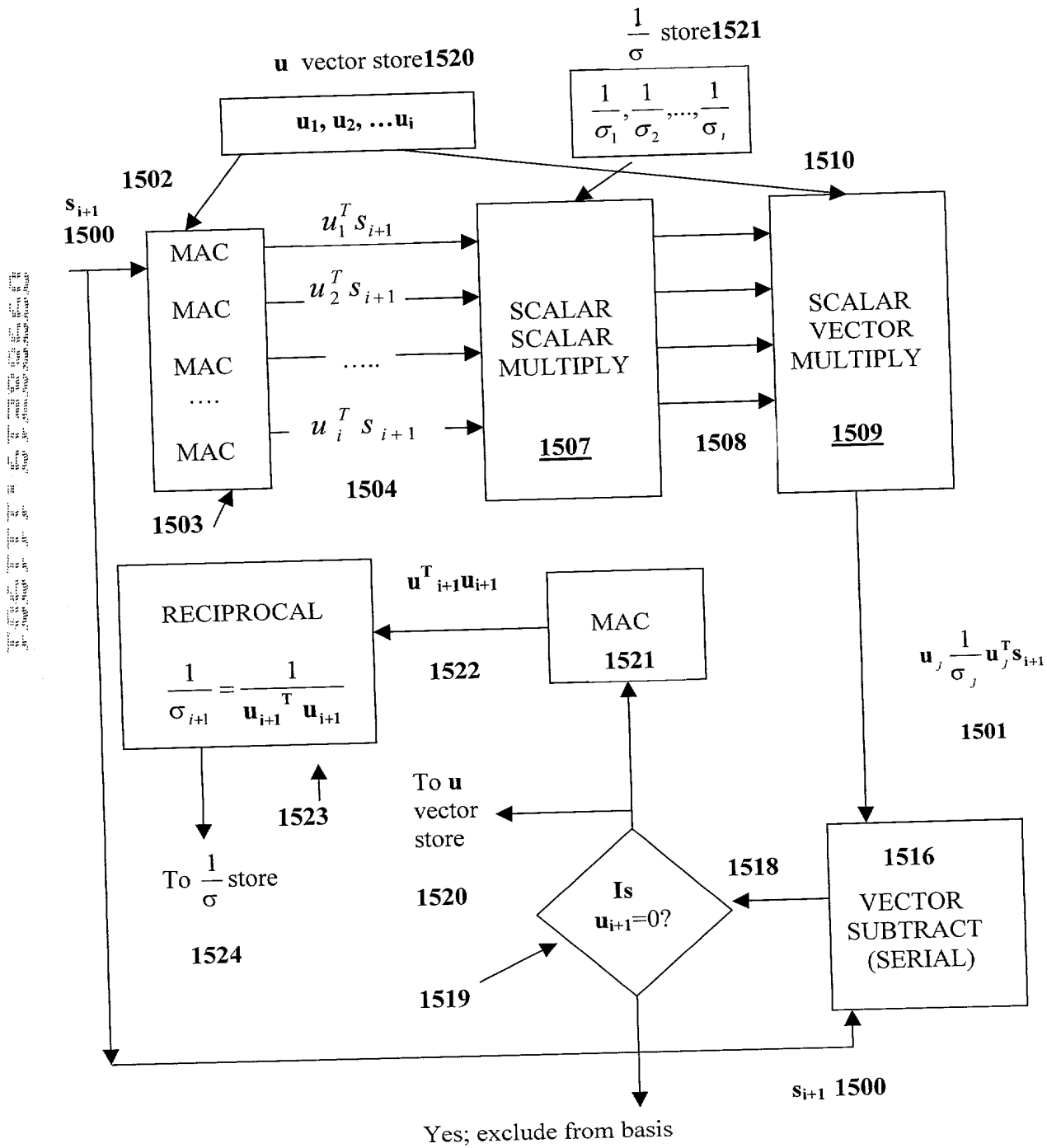


FIG. 15



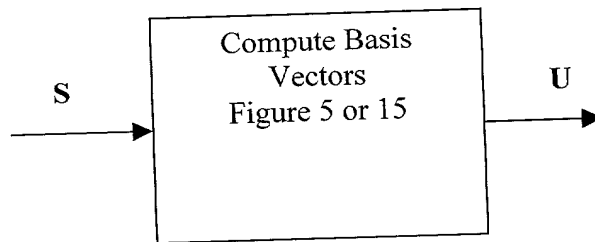
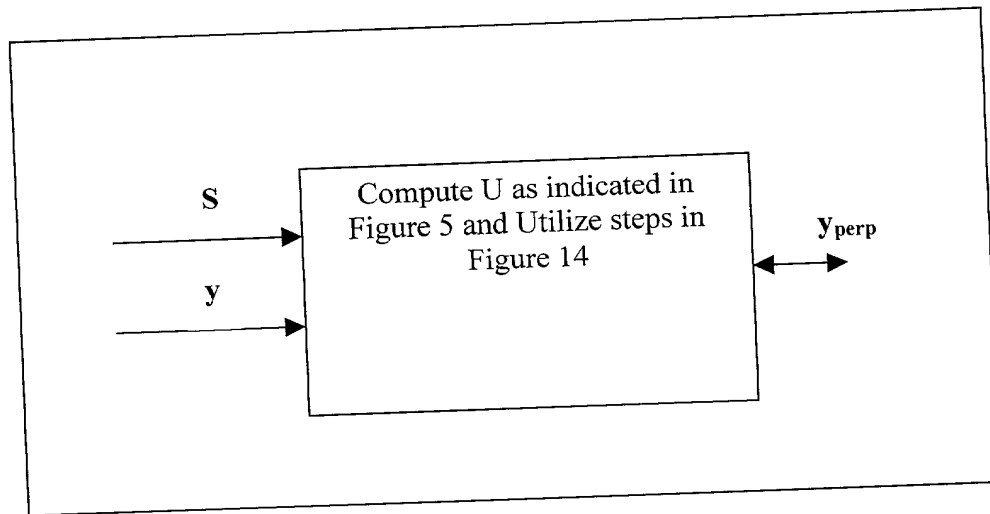
**FIG. 16**



FIG. 17



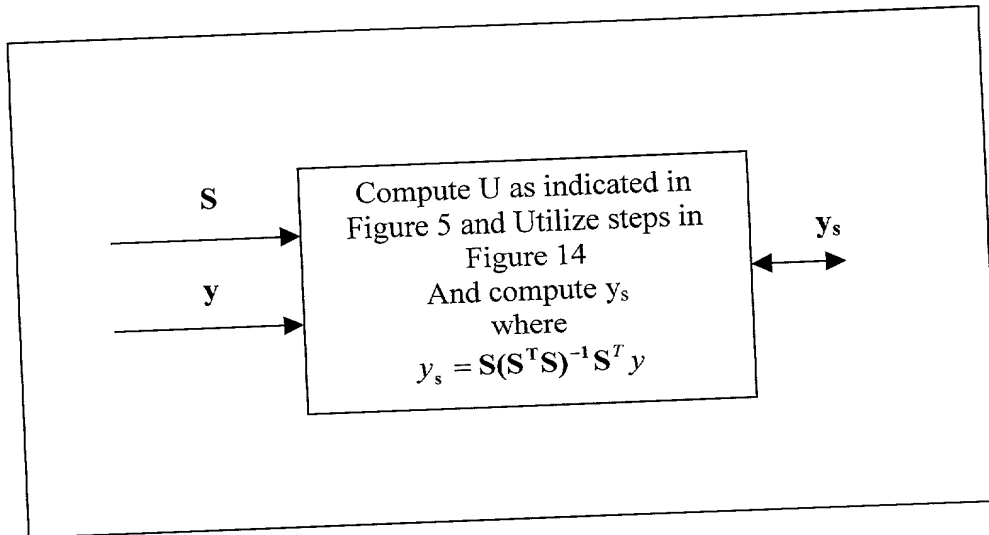
**FIG. 18**

FIG. 19

